

Knowledge Systems and Risk Management: Threat Lessons Learned from COVID-19 in 2020-21

Murray E. Jennex
West Texas A&M University
mjennex@wtamu.edu

Alexandra Durcikova
University of Oklahoma
alex@ou.edu

Ilona Ilvonen
Tampere University
Ilona.ilvonen@tuni.fi

Abstract

The year 2020-21 has shown us that the likelihood of extreme events is greater than we would have expected. When organizational resources are stretched to their limits due to extreme events, they are also more vulnerable to cyber-attacks and knowledge risks. Based on the events that took place during the 2020-21 period, we identify five knowledge risks and categorize them as technical, behavioral, and legal risks. We identify possible controls to mitigate these knowledge risks: proper knowledge identification, guidelines for employee knowledge behavior, identification and evaluation of online communication channels, and risk re-assessment to knowledge.

1. Introduction

2020 was a year of upheaval and unrest that is still impacting us in 2021 [10]. COVID-19 swept the world and shut down many countries across the globe. In addition to COVID-19, the United States had experienced a wide variety of difficulties, such as widespread civil strife with rioting in many cities beginning in the spring of 2020; multiple natural disasters such as several large wildfires in California and a severe hurricane season that affected the southeast United States and a record polar freeze that knocked out the Texas power grid during record freezing temperatures in the winter of 2021, a controversial presidential election, multiple cyber attacks that affected hospitals, financial systems, and production systems in food process and gas pipeline transport; widespread misinformation campaigns about the election and the COVID-19 vaccine [27].

To combat COVID-19 the United States and much of Europe and Asia shut down most of its business operations. The issue of communication and how to conduct work and everyday life came at the center of attention. Social media (Facebook, Instagram, TikTok, etc.) and collaboration systems (Zoom, Teams) enabled communications between large numbers of people with little content moderation that resulted in the spread of

misinformation and the increase of cyber-attacks via phishing and social engineering, and traditional communication.

An additional impact of the shutdown was the loss and/or transience of employees. Many businesses had to lay off employees when they couldn't continue operations. This situation caused a loss of knowledge flow from departed employees and loss of knowledge sharing among remaining employees. As operations are resuming businesses are suffering from not being able to entice former employees to return or to hire new, experienced employees.

During the lockdown, organizations and businesses used knowledge systems (defined later) to manage the storage, retrieval, and application of business knowledge that had to be remotely accessed by employees. A major task that businesses needed to prepare for was to defend their knowledge systems (to some degree) from cyber threats using best practices and risk assessment such as:

- Protect their boundaries, repositories, and equipment.
- Monitor for and respond to attacks and intrusions.
- Monitor and guard against phishing and other social engineering attacks.
- Be prepared for disaster response/business continuity.

Organizations and businesses also reduced risk to their knowledge systems by monitoring and guiding remote users in how to connect, what systems can be used, online behavior rules, and even how to configure the employees' home computers. However, businesses were not prepared for the large-scale remote access and remote system use experienced in the last year.

While there were many traditional security issues that businesses faced during the shutdown, this paper is not about those issues. Our analysis focuses on threats we haven't thought so much about when the shutdown started. However, these threats are now better understood and must be mitigated [27]. We list these threats here:

- Impact of misinformation (primarily on decision making)
- Impact of disinformation (primarily on decision making)
- Impact of social media (primarily on disclosure and knowledge transfer and organizational impact but not the traditional threats from social media)
- Impact of social isolation (primarily on decision making and knowledge transfer)
- Impact of social justice movement (primarily on knowledge transfer through organizational culture)

Research have discussed generic set of knowledge risks [16], however we do not yet understand the how the risks listed above affect knowledge. Thus, this paper discusses knowledge systems and their risks based on published surveys and reports that focus on the issues observed during the COVID-19 pandemic.

2. Background

2.1 The year 2020

The year 2020 has been a difficult year for every country because of the global pandemic caused by COVID-19. As of May 30, 2021, the United States Center for Disease Control reports that the United States has had 33,079,543 cases of COVID-19 with 591,265 reported deaths as of May 30, 2021 [34]. Worldwide, Wikipedia (based on Johns Hopkins data) reports there have been 170,353,921 cases of Covid-19 with 3,541,795 deaths [39].

Businesses ceased having workers come to the office, schools quit holding in-person classes, restaurants/gyms/clubs/ beaches/parks anywhere people gathered or interacted were shut down, and hospitals and medical facilities quit treating anything but COVID and emergency cases. To survive, businesses, organizations, and schools as quickly as possible went online with some of the following outcomes:

- Workers and students spent extended time working remotely outside of the business, organization, or school networks [17].
- Businesses, organizations, and schools moved business processes online.
- Payment systems went touchless/contactless.
- Tools such as Zoom, and Teams were quickly adapted and put into use [17].
- Travel and supply chains were disrupted
- Social systems/networks such as Facebook, YouTube, Instagram, and Tik Tok became the primary means of social interaction and sources of information.
- Most face-to-face communication outside of immediate family units ceased.

Remote work caused employees to communicate with others whom they didn't know in a virtual environment that significantly reduced body language feedback and influence by organizational/corporate behavior rules with the following outcomes:

- COVID-19, social, and election misinformation and disinformation were/are rampant.
- Social justice/change and upheaval have caused great uneasiness in organizations and with and between employees with many being afraid to express thoughts or opinions for fear of being "canceled."
- Social engineering/phishing attempts have become the prevalent cyber-attack vector [6].

However, the year 2020 and early 2021 presented organizations and companies not only with remote work issues but also increased cybersecurity attacks and threats. Before we start our analysis of the knowledge systems, we will define all the terms for more clarity of the explanations provided.

2.2 Definitions of terms used

Misinformation - is false, inaccurate, or misleading information that is communicated regardless of an intention to deceive. [40]. Managing the spread of misinformation has become a contentious issue due to who decides what is misinformation, what is an opinion, and what is truth.

Disinformation - false information, which is intended to mislead, especially propaganda issued by a government organization to a rival power or the media [41]. Disinformation is a subset of misinformation with the key difference being the intent to deceive.

Knowledge - Evolving mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experience into corporate decision making [7]. Knowledge is what is used to support decision-makers.

Knowledge Transfer - refers to the sharing or disseminating of knowledge by a knowledge creator [1]. Knowledge transfer is important in knowledge systems and relies on trusted creators of knowledge moving that knowledge to repositories where it can be retrieved and used by knowledge users.

Knowledge System/Knowledge-Based System - a system that captures and uses knowledge from a variety of sources to assist users with solving problems, particularly complex issues, using tools such as AI, Big Data, DSS, knowledge retrieval, etc. These systems are primarily used to support human decision-making, learning, and other activities [22]. This paper uses the term Knowledge Systems interchangeably with Knowledge-Based Systems.

Risk - the net negative impact of the exercise of a vulnerability considering both the probability and the impact of occurrence [23]. The impact of occurrence can be more broadly considered a hazard, an uncertainty, or an opportunity [5]. Viewing risk as something more than a hazard is highly applicable to knowledge systems [15]. Although KM risks can lead to negative results, they can also represent significant opportunities for learning or new knowledge applications. Uncertainties connected to knowledge systems can be a threat to efficiency, but also an opportunity for innovations [16]. In this paper we examine the events from 2020-21 in light of this broad understanding of risk as not only threats, but also as uncertainties and opportunities.

2.3 Knowledge system risk assessment

Assessing cybersecurity in the organization starts with risk assessment. Jennex and Durcikova [16] discuss risk and threat assessment specific to knowledge systems and build the theoretical foundation for knowledge system threat assessment. In this paper we apply this foundation in analyzing the events of the recent year 2020-21.

The knowledge system risks are assessed by using the KSRM approach of Ilvonen et al. [12] for knowledge security risk management. Ilvonen et al. [12, p.13] define knowledge security “as the managerial process of organizations to identify threats toward important knowledge and secure the knowledge against those threats.”

The point of interest in this definition is important knowledge: knowledge that is important to the organization needs to be identified in all the forms and locations that it resides in, for the organization to be able to do any risk management measures with it. The knowledge risk assessment process thus begins with the identification of knowledge assets by recognizing not only the documented knowledge within different systems of the organization, but also the ways of knowledge sharing and transfer and the role of people and tacit knowledge within the knowledge system.

Jennex and Durcikova [16] present a set of knowledge system specific generic threats. The six generic threats are:

- Failure to identify and capture critical knowledge in the knowledge creation process.
- Not having knowledge creation, capture, and use aligned with organizational strategy.
- Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes.
- Losing critical knowledge by not capturing it from critical human sources.

- Losing critical knowledge by not storing it on nonvolatile media or by not migrating knowledge with changing storage standards or by not meeting legal standards for storing critical knowledge.
- Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge.

Jennex and Durcikova [16] provided an in-depth discussion and many examples of how the above threats impact knowledge systems. However, in 2020-21, because of COVID-19, natural disasters, social upheaval, misinformation, etc. generated more uncertainty and stress overall in organizations and individuals than had been previously experienced since perhaps the great depression.

The uncertainty associated with knowledge use, be it due to rapidly changing technology and storage media, to misuse or new and unexpected uses of knowledge, or the basic understanding of the captured knowledge, is one of the biggest challenges a knowledge system manager faces. To understand the impact of this uncertainty and stress, events, and outcomes from 2020 and 2021 have been analyzed in the following section using the above knowledge system threats and the previously discussed process.

In addition to identifying the important knowledge of an organization, risk assessment requires the understanding of where the threats can enter the organization and target the knowledge system. We use three threat vectors in this paper: technical, behavioral, and legal [16].

3. Analysis of events and observations of 2020-21

Obasiolu [24] found the biggest lesson from 2020-21 to be that security starts from within an organization, meaning that security starts with top management creating a security culture and expectations of behavior. While we agree with this observation, we are providing additional and more concrete observations:

Misinformation/disinformation leads to bad individual decision-making on which links to click or which email to open (KnowBe4 says 88% of data breaches are caused by human error due to phishing and other errors). The largest Twitter and Facebook hacks in 2020 was caused by Twitter and Facebook employees falling for a phishing attack [10] [35].

- Misinformation/disinformation impacts procedural decision-making on hiring, purchasing, and customer service. This can lead to security issues such as internal threats, transferring funds to the wrong bank, and offending customers [20].

- Hundred-year storms (Texas recently, southeast over the late summer, California wildfires) challenge disaster recovery plans and potentially lose knowledge and influence the availability of systems [2] [11] [33].
- A pandemic causes larger than expected personnel turnover and knowledge loss degrading organizational performance
- Organizational culture changes lower trust among workers resulting in less knowledge sharing and most importantly, less sharing of knowledge critical to decision making affecting security (bad sites, hacking attempts, social engineering, etc.)
- Organizational members upset at culture changes deliberately do not share knowledge or share disinformation leading to bad decision making
- Social isolation slows the sharing, capturing, and reuse of knowledge needed for security decisions
- Social isolation increases the use of social media leading to more potential disclosures, more opportunities for downloading malware onto worker computers used for home and work, lower filters to determining misinformation/disinformation [35].
- Generation Z is most impacted by the above issues [29].

These observations are analyzed in this section using five of the previously listed knowledge system threats and the above-mentioned threat vectors. The threat of not having knowledge creation, capture, and use aligned with organizational strategy is only mildly impacted so is not addressed.

3.1 Failure to identify/capture critical knowledge in the knowledge creation process in 2020-21

With most workers working remotely, decision-making was automatically pushed down to them. Being remote made it difficult for workers to stay current in the knowledge needed to support decision-making. Also, remote work creates isolation from work networks which in turn slows the spread of knowledge and enables the spread of misinformation and disinformation. Remote work makes workers more susceptible to not being able to identify misinformation and disinformation and making wrong decisions as to what is critical knowledge. A focus on COVID-19 may lead organizations and workers to not keeping automated tools up to date and collecting critical knowledge. Finally, the rapid spread and use of new collaboration tools such as Zoom and Teams [17] could have led organizations to not integrate these new tools into automated knowledge capture tools so new

knowledge generated and spread by these new collaboration tools may not be captured.

Technical threats are from the quick adoption of new collaboration technologies such as Zoom and Teams [17] with subsequent slow integration into organizational systems and potential for automated tools not working with the new technology.

Behavioral threats are from widespread remote work and worker isolation and a flood of misinformation/disinformation pushed to socially isolated workers [20]. This increases the likelihood of missing critical knowledge and identifying misinformation and disinformation as critical knowledge.

Legal threats are stemming from new privacy laws (e.g., California) as well as a myriad of new social justice, health, and diversity/inclusion mandates greatly increasing the risk of missing a legal requirement for capturing critical knowledge, not protecting critical knowledge, or identifying incorrect critical knowledge.

3.2 Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes in 2020-21

With widespread remote work, social isolation, and greatly reduced supervision humans replace normal socialization with online socialization [21]. With reduced supervision, malicious/hacktivist employees were more likely to disclose or commit fraud [20] greatly increasing the likelihood that critical knowledge will be disclosed. Social isolation makes humans more vulnerable to social engineering. New group/collaboration software increases the reach of social engineers including nation-state social engineers. Many instances of over disclosure were revealed this last year in Zoom and Twitter attacks.

Technical threats are stemming from the exploitation of communication vulnerabilities common to all communication systems and are focused on communication processes specific to knowledge systems. Additional threats are from storage media that does not properly secure access to cloud storage and/or server storage. 2020 increased these threat likelihoods because organizations quickly adopted collaboration software while not having the onsite staff to supervise and monitor installations and updates. Examples of these threats include Zoombombing [8] and large-scale hacks at Twitter.

Behavioral threats are come from intentionally or accidentally failing to maintain access control lists for authorizing approved personnel to access knowledge, posting knowledge to inappropriate forums, not following disclosure processes, not encrypting knowledge in motion, falling victim to social

engineering attacks, and either disclosing knowledge to unauthorized individuals or allowing malware onto their systems that are collecting and transmitting knowledge to unauthorized individuals [6]. 2020 saw this threat likelihood greatly rise by increasing the attack surface through social isolation and widespread remote workers [20] [35] [36]. Additionally, workers were not able to create quality relationships with new organizational members as they could only meet remotely [20]. Examples of behavioral threats include social engineering attacks on Twitter [8] [35] that had workers responding to disinformation.

Legal threats come from intentionally or accidentally not complying with disclosure laws such as those dealing with personally identifiable information or patient health knowledge. 2020 saw new privacy laws in California as well as a myriad of new social justice, health, and diversity/inclusion mandates greatly increasing the risk of missing a legal requirement.

3.3 Losing critical knowledge by not capturing it from critical human sources in 2020-21

The pandemic has forced societies to shutdowns and many organizations have severely reduced or even ceased operations or changed their operations to purely online environments. As organizations strive for survival, they have been forced to lay off a lot of employees rapidly, discard a lot of old technology and rapidly adopt new technological tools. In addition to layoffs, there have been extended absences due to long-term illness and unanticipated deaths of employees. All of these have resulted in losing critical knowledge.

Technical threats are linked to not being able to utilize established tools and processes for capturing knowledge from departing personnel. 2020-21 saw rapid shutdowns and employee loss that precluded organizations and companies from using their knowledge capture tools and processes to capture knowledge from laid-off employees. Additionally, COVID-19 caused large numbers of deaths where most of these deaths occurred in isolated wards that also precluded any possibility of capturing knowledge before the employee's death.

Another threat is from ransomware encrypting critical knowledge repositories and the organization or company not being able to recover them through backups or by paying the ransom. Some major examples include JB Swift paying approximately \$11 million [3] and the Colonial Pipeline approximately \$5 million to retrieve their data [28] while the University of California, San Diego paid \$1 million ransom to

ensure their COVID-19 research data was not destroyed [42]. 2020-21 increased the likelihood of the above threats especially due to the quick adoption of new technologies and procedures while eliminating older technologies and procedures.

A final threat comes from wildfires, polar blasts, hurricanes, and flooding all of which challenged disaster recovery/business continuity plans as remote workers couldn't or had difficulty accessing backup and recovery systems to support implementing the recovery and thus returning captured critical knowledge to organizational/company use.

Behavioral threats come from intentionally or accidentally not identifying critical human knowledge repositories and taking actions to capture and store the critical knowledge (e.g., not capturing knowledge from retiring personnel but also can occur by not capturing knowledge from personnel departing an organization for reasons other than retirement). 2020 saw increased employee stress as organizations changed how they were operating. As new systems/processes were implemented, the likelihood of knowledge loss increased. Knowledge was lost as employees were suddenly let go, got sick, or even died. Social isolation and loss of trust in the organization have reduced knowledge sharing and knowledge capture. Misinformation/disinformation has created confusion as to what was the knowledge needing to be captured.

Legal threats originated from intentionally or accidentally not complying with required knowledge capture (an example of this was Nuclear Regulatory Commission requirements on nuclear stations to capture critical knowledge from employees before large-scale workforce layoffs). 2020 has lowered the focus on capturing knowledge from departing employees as organizations struggle just to survive, and this is likely to become an issue in the long term, even if it has not been an issue in the short term.

3.4 Losing critical knowledge by not storing it on nonvolatile media/not migrating knowledge with changing storage standards/not meeting legal standards for storing critical knowledge in 2020-21

While COVID-19 did not directly impact this outcome, not having personnel in the office means migration of data to newer technologies was slow or non-existent. Natural disasters were wreaking havoc, though, like California and Australian wildfires, Texas polar blast, and hurricanes, and flooding in the southeast United States have impacted power and communication grids which in turn impacted secure storage facilities [11] [38].

Technical threats are rooted in the failure of storage media, hardware, and/or software. Additional threats are from technical obsolescence leading to the loss of knowledge as the organization migrates to newer technologies or from the failure of obsolete devices. Other threats come from the loss of repository devices and not having an appropriate backup process in place or an installed tracking system. A final threat is from ransomware encrypting critical knowledge repositories and not being able to recover them through backups or by not paying the ransom. 2020-21 saw many successful ransomware attacks that resulted in large payouts (see section 4.3 for examples). Additionally, events that cause widespread damage or extended loss of power can cause storage devices to fail or be destroyed. 2020-21 saw a 100+ year winter storm that caused the grid to fail in the state of Texas [33], wildfires in California [2] and Australia [11] that destroyed miles of transmission lines and equipment, and record hurricanes and storms in the southeast United States [11] that also destroyed miles of transmission lines and equipment. The technical threats come from failed equipment and backups and security teams need to review their disaster recovery/business continuity plans to ensure the secure storage being counted on is truly secure from a power and communication point. Note that Y2K had many of the same issues and it was important that the work on Y2K was done as it was much worse than the public knew.

Behavioral threats are from intentionally or accidentally not following technology procurement processes, selecting providers without checking their technology, not planning for obsolescence, not testing technologies before applying them or while using them, and/or artificially obsoleting technologies before age requires it. 2020-21 saw great disruptions in supply chains and in purchasing decisions so this threat likelihood was greatly increased. Additionally, remote workers were more likely to not follow backup processes due to lack of system access or not being able to while following new processes.

Legal threats are from liability issues associated with not following sanctioned or committed storage standards (such as those standards from NIST and ISO). 2020-21 saw remote work with many office locations not staffed, this increases the likelihood of this occurring as IS/IT staff can't migrate to new storage standards or make changes to existing storage standards.

3.5 Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge in 2020-21

This is perhaps the most likely threat given the proliferation of misinformation and disinformation. The response to COVID-19 is replete with this happening with perhaps the most egregious example being that of deciding to send COVID-19 patients to nursing homes so that they could get better care but, in the process, infecting the most vulnerable. The most recent example is on those deciding not to get the vaccine. The main issue was the proliferation of misinformation and disinformation in virtually every aspect of the 2020-21 issues. There is misinformation and disinformation in COVID-19, the 2020 elections, the social justice movement, and virtually every other issue. In addition to misinformation and disinformation, there are new processes for identifying and censoring misinformation and disinformation. Finally, remote workers have access to all this misinformation and disinformation but do not have support in determining what is true and what is false as the media in the United States has become politicized and partisan and while the social media firms are making attempts to censor misinformation and disinformation, creating their censor rules on the fly.

Technical threats are from search tools not finding relevant knowledge, improperly prioritizing some knowledge, not using integration tools allowing relevant knowledge to not be incorporated into search results, and/or using visualization technologies that influence decision-makers to the wrong option. 2020-21 saw the rise of the use of AI tools to filter out misinformation and disinformation. However, the problem with AI tools is that they reflect the bias of their builders, and this was obvious with the tools used by Facebook, Twitter, YouTube, Google, etc. Additional threats come from the classification of knowledge in knowledge systems and this effort being slowed by workers working remotely and not having access to all the knowledge gathered or the time to solicit and classify knowledge from other remote workers. A final threat comes from knowledge systems not having adequate processes for validating the accuracy of knowledge in the system.

Behavioral threats are from decision-makers using incomplete knowledge, and/or inappropriately applying knowledge to unsuitable decision contexts. 2020-21 saw this likelihood greatly increased as social isolation, social media use, and lack of interactions with organizational experts increased while reliance on media fact-checkers led to an increased likelihood of using weak/bad knowledge for making decisions.

Legal threats are from decision-makers not utilizing due care or due diligence in assessing knowledge and focusing on politically correct or desired advice. Another threat is from not giving advice or giving advice based on limiting liability rather than stating the advice suggested by the knowledge system. 2020-21 saw a great increase in social unrest leading to whole new standards and laws on social justice and revised history greatly increasing the likelihood of this threat. While not quite a legal issue (it is vigilante justice), society has taken to “canceling” individuals and organizations that don’t support new norms. Knowledge systems have the risk of not changing content fast enough to avoid not meeting new norms, which has resulted in canceling of organizations and companies.

4. Discussion

The purpose of this paper was to analyze risk to knowledge in the light of the recent COVID-19 pandemic. Obasiolu [24] reports that companies did not know themselves well enough to implement a security program resilient enough to handle the many severe challenges faced in 2020-21. An organization cannot properly secure its knowledge assets if it doesn’t understand its main business processes and validation of these processes that create knowledge. The Organization for Economic Cooperation and Development (OECD) [25] reports that cybersecurity risks greatly increased in crises because stressed organizations and companies are more vulnerable to attacks. This paper agrees with this assessment and describes further threats for knowledge systems and knowledge system risk assessment under extreme circumstances as created by COVID-19 and other natural disasters during 2020 and 2021. We identified five specific cases of knowledge risk and described them in terms of technical, behavioral, and legal threats.

There are several critical issues that every organization must address. First is the issue of knowledge identification, more specifically identifying misinformation and disinformation. Organizations can address this threat by training employees in how to identify misinformation/disinformation [38], or by creating a position that would be responsible for monitoring and identifying misinformation/disinformation [18]. The usage of AI tools for filtering news, emails, for identifying deep fakes, frauds, misinformation/disinformation will be critical for an organization to be able to make good business decisions using validated knowledge sources. Finally, organizations need to find a way to inform their employees about misinformation/disinformation,

frauds, and deep fakes, while not overburdening them with additional information.

The second is forming or rewriting guidelines and instructions for employee online behavior. Organizations need to focus on the social media usage of their employees for both knowledge sharing and knowledge reuse. The dilemma that organizations are facing is how to create rules that create acceptable social media usage without denying freedom of speech. Future research should evaluate the limit of what is acceptable and unacceptable to talk about on social media when it comes to organizations and their lives. There is a need to define the protocols of responding to questions in social media; for example, when an employee responds, should his/her view be treated as the views of the organization or personal views? Guidelines about social media engagement during and after work hours are needed specifically for the remote workforce because of the blurry line between work and private life. The guidelines for social media engagement should also include a section on how to spot and evaluate potential misinformation and disinformation, as well as the threat of downloading malware.

The third is the identification and evaluation of communication channels. The social isolation of employees creates a unique problem. We have learned that employees miss socializing with their coworkers and that virtual social hours do not work as a replacement for physical socializing. Especially Generation Z is very sensitive to social isolation and organizations need to create special networking programs for these employees. Promoting socializing channels that help people to get together and know each other helps the organization to reduce the risk of employees falling prey to social engineering attacks. Correct channels for work-related socializing also reduce the risk of knowledge spillovers, as well as helps promote job satisfaction among the employees, and thus reduce unwanted employee turnover.

Finally, a major risk re-assessment is needed in most organizations. Extreme disasters (wildfires, riots, floods, hurricanes, polar blasts, etc.) cause major disruption in the operations of a business. Organizations need to come up with strategies to secure knowledge when a natural disaster hits and when it may destroy knowledge sources or access to these knowledge sources might not be available. Re-evaluation of disaster response/business continuity plans is needed given that the likelihood of extreme events is much higher than most organizations anticipated even a year ago. Knowledge systems that allow employees to share and retrieve knowledge must be not only defended against natural threats but also be easily accessible while working remotely.

5. Conclusions

2020-21 may be outlier years but it has shown us that the likelihood of extreme events is greater than we like to admit. We must acknowledge that organizations are more vulnerable to cyber-attacks when stressed [25], and other knowledge risks are also compounded when the environment of the organization is in turmoil.

Parakilas [27] suggests expanding the definition of the cyber threat to include more than just traditional and terrorist attacks. This paper expands the threats to knowledge systems to include the wide variety of issues discussed in the paper. However, these threats are outside the technical expertise of the traditional cybersecurity department. Taking a wider perspective to the risks to the knowledge systems and their use in the organization, seemingly small technical risks may turn out to be big risks to smooth daily operation and knowledge transfer. Cybersecurity organizations need to be agile [25] interdisciplinary in composition and include experts in knowledge capture, transfer, and use as well as in decision making.

Expertise in identifying and countering misinformation/disinformation is also needed in the cybersecurity organization [38]. Identifying important knowledge in the organization is not an easy feat, as this requires the understanding of knowledge transfer and retrieval processes of employees, and their practices of evaluating the knowledge they have access to. It thus is not enough for the organization that the cybersecurity experts are able to identify misinformation on sight. They need to know how misinformation and disinformation reach the employees and help the employees to spot them as well. This cannot be only the task of security professionals, rather, the involvement of the whole of the organization is needed.

Finally, organizations and companies need expertise in organizational psychology to assist the organization in preparing employees to understand, identify, and deflect/reject misinformation, disinformation, and phishing [36] and to aid in identifying the insider threat. Another value from having organization psychology expertise is in assisting employees in dealing with anxiety related to remote work and social justice issues. The bottom line is that the human element must be addressed first in cybersecurity [35].

6. References

[1] Alavi, M. and Leidner, D.E. (2001) Review: Knowledge Management and Knowledge Management Systems:

Conceptual Foundations and Research Issues, *MIS Quarterly*, 25(1), 107-136.

[2] Alonso, M. and Sanchez, R., (2020). California's record-breaking wildfires consume nearly 1 million acres in a month. CNN, October 17, 2020. Retrieved on June 11, 2021, from <https://www.cnn.com/2020/10/17/us/california-wildfires-saturday/index.html>

[3] Associated Press, (2021). Meat company JBS confirms it paid \$11M ransom in cyberattack. Associated Press, June 10, 2021. Retrieved on June 12, 2021, from <https://www.usatoday.com/story/tech/2021/06/10/jbs-confirms-paid-11-million-ransom-cyberattack/7633299002/>

[4] Aubert, B., M. Patry, and Rivard, S. (1998). "Assessing the Risk of IT Outsourcing," Proceedings of the 31st Hawaii International Conference on Systems Sciences. IEEE Publishing, 685 – 693.

[5] Billington, J. (1997). "A Few Things Every Manager Ought to Know About Risk," *Harvard Management Update*, 2(3), March, pp. 1-12.

[6] Columbus, L. (2021). Top 10 cybersecurity lessons learned one year into the pandemic. *VentureBeat* March 11, 2021. Retrieved June 10, 2021, from <https://venturebeat.com/2021/03/11/top-10-cybersecurity-lessons-learned-one-year-into-the-pandemic/>.

[7] Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

[8] Downs, F., (2021). Major Lessons to be Learned from 2020 Security Mishaps. *InfoSecurity Magazine*. Retrieved June 10, 2021, from <https://www.infosecurity-magazine.com/blogs/major-lessons-learned-2020-mishaps/>

[9] FitzGerald, J., A. Dennis, A. Durcikova, "Business Data Communications and Networking," Wiley, 13th Edition (2017)

[10] Gat Labs, (2020). The Biggest Cloud Security Lessons Learned in 2020 (A Year in Review). Gat Labs Blog. Retrieved June 10, 2021, from <https://gatlabs.com/blogpost/cloud-security-lessons-learned-in-2020/>

[11] Gramling, C., (2020). Wildfires, heat waves and hurricanes broke all kinds of records in 2020. *Science news*, December 21, 2020. Retrieved on June 11, 2021, from <https://www.sciencenews.org/article/climate-change-wildfires-heat-waves-hurricanes-records-2020>

[12] Ilvonen, I., Jussila, J. J., & Kärkkäinen, H. (2015). Towards a business-driven process model for knowledge security risk management: Making sense of knowledge risks. *International Journal of Knowledge Management (IJKM)*, 11(4), 1-18.

[13] ISO 27001:2013 (reviewed 2019) Information technology -- Security techniques -- Information security management systems – Requirements, International Standards Organization.

[14] ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management, International Standards Organization

[15] Jennex, M.E. and Durcikova, A. (2014). "Integrating KM and Security: Are We Doing Enough?" *International Journal of Knowledge Management*, 10(2), pp. 1-12.

[16] Jennex, M. E., & Durcikova, A. (2020). Creating Sustainable Knowledge Systems: Towards a Risk and Threat

- Assessment Framework. *Journal of Strategic Innovation and Sustainability*, 15(4). <https://doi.org/10.33423/jsis.v15i4.2965>
- [17] Kelly, R., (2021). How the Pandemic Boosted Ed Tech Adoption. *Campus Technology*, June 8, 2021. Retrieved on June 14, 2021 from https://campustechnology.com/articles/2021/06/08/how-the-pandemic-boosted-ed-tech-adoption.aspx?s=ct_nu_150621&oly_enc_id=6899H3366067E5A
- [18] Levick, R., (2021). Should Companies Consider Appointing Chief Paranoia Officers to Combat Disinformation? *Brink*, February 21, 2021. Retrieved June 10, 2021, from <https://www.brinknews.com/should-companies-consider-appointing-chief-paranoia-officers-to-combat-disinformation/>
- [19] McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology*. CRC Press.
- [20] Nabe, C., (2021). Impact of COVID-19 on Cybersecurity. *Deloitte*. Retrieved on June 11, 2021, from <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html#>
- [21] Newcloud Networks, (2021). The Impact a Pandemic Can Have on Cybersecurity. *Newcloud Networks*, February 3, 2021. Retrieved on June 11, 2021, from <https://blog.newcloudnetworks.com/the-impact-a-pandemic-can-have-on-cybersecurity>
- [22] Nissen, M., (2002). An extended model of knowledge-flow dynamics. *Communications of the Association for Information Systems*, 8(1), 18.
- [23] NIST SP 800-37 rev 2, (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, National Institute of Standards and Technology, retrieved June 8, 2019 from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- [24] Obasiolu, D., (2020). Important Cybersecurity Lessons Learned During the Pandemic. *Forbes*, November 2, 2020. Retrieved June 10, 2021, from <https://www.forbes.com/sites/theyec/2020/11/02/important-cybersecurity-lessons-learned-during-the-pandemic/?sh=4941e9117aa9>
- [25] Organization for Economic Cooperation and Development, OECD, (2020). Seven lessons learned about digital security during the COVID-19 crisis. *OECD*, November 4, 2020. Retrieved on June 10 from https://read.oecd-ilibrary.org/view/?ref=137_137440-yavecbtye4&title=Seven-lessons-learned-about-digital-security-during-the-COVID-19-crisis
- [26] Padyab, A. M., Päiväranta, T., & Harnesk, D. (2014). Genre-Based Approach to Assessing Information and Knowledge Security Risks. *International Journal of Knowledge Management*, 10(2), 13-27.
- [27] Parakilas, J., (2020). The Lesson of 2020? Security Doesn't Mean What You Think It Does. *The Diplomat*, December 23, 2020. Retrieved on June 10, 2021, from <https://thediplomat.com/2020/12/the-lesson-of-2020-security-doesnt-mean-what-you-think-it-does/>
- [28] Shear, M.D., Perlroth, N., and Krauss, C., (2021). Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers. *New York Times*, June 7, 2021. Retrieved on June 12, 2021, from <https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html>
- [29] Sherr, I., (2021). Gen Z is getting screwed by remote work, Microsoft survey finds. *CNET* March 22, 2021. Retrieved on June 10, 2021, from <https://www.cnet.com/news/gen-z-is-getting-screwed-by-remote-work-new-microsoft-survey-says/>
- [30] Smith, T.A., Mills, A.M., & Dion, P., (2010). Linking Business Strategy and Knowledge Management Capabilities for Organizational Effectiveness. *International Journal of Knowledge Management*, 6(3), pp. 22-43.
- [31] Spears, J. (2012). Conceptualizing Data Security Threats and Countermeasures in the E-Discovery Process with Misuse Cases. *AMCIS 2012 Proceedings*. Paper 17. <http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/17>
- [32] Thalmann, S., Manhart, M., Ceravolo, P., & Azzini, A. (2014). An integrated risk management framework: measuring the success of organizational knowledge protection. *International Journal of Knowledge Management (IJKM)*, 10(2), 28-42.
- [33] Timmer, J., (2021). Texas' power grid crumples under the cold. *ARS Technica*, February 15, 2021. Retrieved on June 11, 2021, from <https://arstechnica.com/science/2021/02/texas-power-grid-crumple-under-the-cold/>
- [34] United States Center for Disease Control, (2021) Covid Data Tracker, retrieved on May 31, 2021 from https://covid.cdc.gov/covid-data-tracker/#cases_casesper100klast7days.
- [35] Vijayan, J., (2020). 6 Cybersecurity Lessons From 2020. *Dark Reading*, November 3, 2020. Retrieved on June 10, 2021, from https://www.darkreading.com/attacks-breaches/6-cybersecurity-lessons-from-2020/d-id/1339333?image_number=1.
- [36] Vodopyan, E., (2021). 2020: IT Security Lessons to Learn. *Netwrix Blog*, June 4, 2021. Retrieved on June 10, 2021, from <https://blog.netwrix.com/2020/12/30/2020-it-security-lessons-to-learn/>
- [37] Walsh, J. P., and Ungson, G. R. (1991). Organizational Memory. *Academy of Management Review*, 16(1), pp. 57-91.
- [38] Weatherford, M., (2021). Misinformation, Disinformation, and what Government can do about them. *Governing*, March 3, 2021. Retrieved June 10 from <https://www.governing.com/security/misinformation-disinformation-and-what-government-can-do-about-them.html>
- [39] Wikipedia, (2021) Covid-19 Pandemic Data. Retrieved on May 31, 2021, from https://en.wikipedia.org/wiki/Template:COVID-19_pandemic_data
- [40] Wikipedia, (2021a). Misinformation. Retrieved on June 6, 2021, from <https://en.wikipedia.org/wiki/Misinformation>.
- [41] Wikipedia, (2021b). Disinformation. Retrieved on June 6, 2021, from <https://en.wikipedia.org/wiki/Disinformation>
- [42] Winder, D., (2020). The University of California Pays \$1 Million Ransom Following Cyber Attack. *Forbes*, June 29, 2020. Retrieved on June 11, 2021, from <https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=48c1c9c818a8>

